Dépannage des terminaux de la gamme Catalyst 9000 ne recevant pas d'adresse DHCP lorsqu'ils sont redirigés par ISE

Table des matières

Problème

Après avoir activé l'authentification à l'aide de la redirection à partir de Cisco Identity Services Engine (ISE) sur un commutateur de la gamme Cisco Catalyst 9000, les points d'extrémité filaires sont par intermittence incapables d'obtenir des adresses IP via le protocole DHCP (Dynamic Host Configuration Protocol). Aucun problème n'est observé sur les commutateurs de la gamme non Catalyst 9000 utilisant les mêmes configurations.

Environnement

- Famille de produits : Gamme Catalyst 9000
- Ordinateurs Windows présentant des échecs d'acquisition DHCP
- La liste de contrôle d'accès (ACL) de redirection sur le commutateur de la gamme Catalyst 9000 ne refuse pas explicitement le trafic DHCP

Résolution

1. Ajoutez les instructions deny suivantes à la liste de contrôle d’accès de redirection pour gérer explicitement le trafic DHCP :

```
deny udp any eq bootps any
```

```
deny udp any any eq bootpc

deny udp any eq bootpc any
```

2. Après avoir modifié la liste de contrôle d'accès, authentifiez à nouveau un périphérique défaillant pour vérifier qu'il peut désormais récupérer une adresse IP via DHCP.

Motif

Lorsque l'authentification est activée, les commutateurs de la gamme Catalyst 9000 traitent les paquets différemment des modèles de commutateurs plus anciens. L'ordre de traitement des paquets sur les commutateurs de la gamme Catalyst 9000 est le suivant :

1. Les paquets qui correspondent à une règle ACE (Access Control Entry) d'autorisation sont envoyés au processeur pour être redirigés vers le serveur AAA.

2. Les paquets qui correspondent à une règle ACE de refus sont transférés via le commutateur.

3. Les paquets qui ne correspondent ni aux règles d'autorisation ni aux règles de refus d'accès sont traités par la liste de contrôle d'accès téléchargeable suivante et, s'il n'existe aucune liste de contrôle d'accès, les paquets atteignent la liste de contrôle d'accès implicite de refus et sont abandonnés.

Cette méthode de traitement diffère des modèles de commutateurs plus anciens qui utilisent des listes de contrôle d'accès par défaut qui autorisent le trafic DHCP par défaut et qui sont traitées avant les listes de contrôle d'accès de redirection. Les modèles de la gamme Catalyst 9000 n'utilisent pas ces listes de contrôle d'accès par défaut et s'appuient entièrement sur les listes de contrôle d'accès de redirection et DACL en place sur la session. La liste de contrôle d'accès par défaut pour les sessions en mode fermé sur les commutateurs Catalyst prédécesseurs est la suivante :

```
3750#sh ip access-lists Auth-Default-ACL

Liste d'accès IP étendue Auth-Default-ACL

    10 permit udp any range bootps 65347 any range bootpc 65348 (22 correspondances)

    20 permit udp any any range bootps 65347 (12 correspondances)
```

```
30 deny ip any any
```

Autres informations utiles

- ACL par défaut pour l'authentification 802.1X
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.